(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
26 juillet 2001 (26.07.2001)

PCT

(10) Numéro de publication internationale
WO 01/54085 A2

(51) Classification internationale des brevets[7] : G07F 7/10

(21) Numéro de la demande internationale :
PCT/FR01/00172

(22) Date de dépôt international :
19 janvier 2001 (19.01.2001)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
00/00664 19 janvier 2000 (19.01.2000) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE** [FR/FR]; 3, rue Michel Ange, F-75794 Paris Cedex 16 (FR).

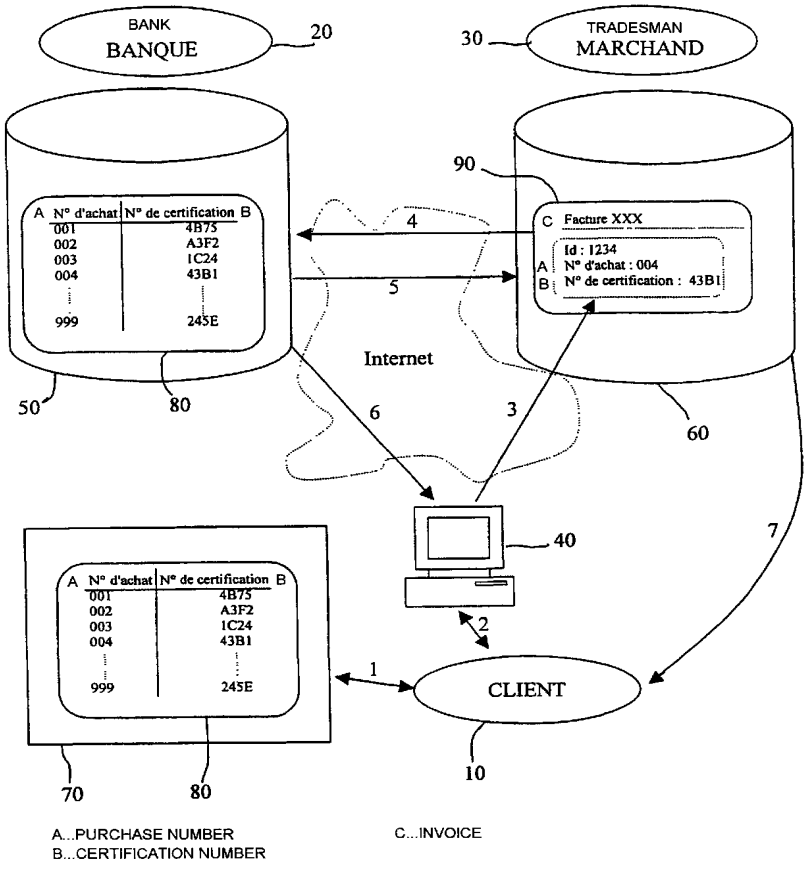
(72) Inventeur; et
(75) Inventeur/Déposant *(pour US seulement)* : **MORET DE ROCHEPRISE, Ghislain** [FR/FR]; 22, allée Albert Thomas, F-91300 Massy (FR).

(74) Mandataires : **ALLANO, Sylvain** etc.; Pontet Allano & Associés SELARL, 25, rue Jean Rostand, Parc-Club Orsay-Université, F-91893 Orsay Cedex (FR).

[Suite sur la page suivante]

(54) **Title:** SYSTEM AND METHOD FOR MAKING SECURE DATA TRANSMISSIONS

(54) **Titre :** SYSTEME ET PROCEDE DE SECURISATION DES TRANSMISSIONS D'INFORMATIONS



(57) Abstract: The invention concerns a system for making secure transactions by mail-order purchasing, in particular on the Internet, with delivery of a unique and non-reusable code for each completed transaction. The system involves a third party (20, 50) between the purchaser (10) and the seller (30, 60). Said third party has a table (80) likewise stored in an electronic fill device (70) of the purchaser (10). The third party validates the purchase when the code, issued from the electronic fill device (70) and transmitted by the purchaser, is identical to a code present in the table located at the third party's. Said code advantageously comprises the value of an incremental counter associated with a certification number randomly determined when the electronic fill device (70) is initialised.

(57) Abrégé : L'invention concerne un système de sécurisation des transactions lors d'achat par correspondance, notamment sur Internet, avec délivrance d'un code unique et non réutilisable pour chaque transaction effectuée. Le système fait intervenir un tiers de confiance (20, 50) entre l'acheteur (10) et le marchand (30, 60). Ce tiers de confiance possède une table (80) également stockée dans un boîtier électronique (70) de l'acheteur (10). Le tiers de confiance valide l'achat

[Suite sur la page suivante]

WO 01/54085 A2

(81) États désignés *(national)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) États désignés *(régional)* : brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Publiée :

— *sans rapport de recherche internationale, sera republiée dès réception de ce rapport*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

lorsqu'un code, provenant du boîtier électronique (70) et transmis par l'acheteur, est identique à un code présent dans la table localisée chez ce tiers de confiance. Ce code comprend avantageusement la valeur d'un compteur incrémental associé à un numéro de certification déterminé de façon aléatoire lors de l'initialisation du boîtier (70).

"Système et procédé de sécurisation des transmissions d'informations."

La présente invention concerne un système et un procédé de sécurisation des transmissions d'informations, et notamment lors de transactions lors d'achats par correspondance, en particulier sur Internet ou Minitel ou par téléphone.

La vente de produits par correspondance, notamment sur Internet, nécessite un système de transmission d'ordre de paiement inviolable. Le principe actuellement le plus répandu est la communication par l'acheteur de ses cordonnées bancaires, via les coordonnées de sa carte de crédit. Ces informations sont de plus en plus souvent transmises cryptées afin d'éviter la fraude. Le cryptage pouvant être effectué soit par le logiciel de navigation Internet, typiquement en utilisant le protocole SSL, soit par un logiciel dédié utilisant un algorithme tel que, par exemple, RSA 128. Il est à noter cependant que tout cryptage est réputé décryptable. Les variables de résolution d'un code de cryptographie sont, en fonction de la complexité du code, la puissance de calcul mis en regard et le temps disponible. Dans de nombreux pays l'utilisation de système de cryptographie très évolué est en outre limité par un cadre législatif permettant aux états de conserver le contrôle si nécessaire de la diffusion des informations. Ainsi l'évolution permanente de la puissance des ordinateurs grand public est elle nécessairement une remise en cause permanente de la qualité des codes de cryptographie.

Cependant la cryptographie ne répond qu'à une seule problématique des transmissions d'informations sur

Internet, à savoir le risque d'interception du message entre les deux acteurs. Or, la confidentialité d'un message doit être complète, en particulier en matière de paiements, de bout en bout de la chaîne. Ainsi il est nécessaire de tenir compte de la bonne foi au niveau du marchand qui, ayant reçu les coordonnées bancaires en clair, aurait la possibilité de les détourner de l'usage prévu par l'acheteur. Un cas courant de fraude est ainsi la lecture sur les tickets de caisses en magasins des éléments des cartes de crédits, en particulier le nom de son propriétaire, son numéro de série, et sa date de validité, éléments que la plupart des services de vente par correspondance considèrent comme suffisant pour valider un achat.

Une autre source d'insécurité en particulier sur les réseaux informatiques, est le vol par effraction de bases de données stockant les informations personnelles des clients d'une entreprise, au nombre desquels leurs numéro de cartes de crédits. En fait, les possibilités de fraudes par piratage informatique ou autre restent réelles tant que le code des cartes bancaires est accepté par les commerçants sans preuve de la légitimité de l'acheteur.

Les alternatives existantes sont tout d'abord le paiement par chèque ou par mandat, bien moins pratiques pour le client, et réfuté par certains commerçants car limitant les achats impulsifs. On trouve ensuite, sur Internet, les solutions basées sur la lecture des informations de sécurisation des cartes bancaires à l'aide de lecteurs de carte. Ce système nécessite de la part de l'acheteur d'être équipé d'un lecteur adapté, ce qui restreint notablement sa liberté d'achat. De plus ce système améliore la sécurité du point de vue du marchant, qui est ainsi assuré de la validité de son acheteur, mais ne change en rien au fait que l'utilisateur, dont le code

de carte bancaire peut être piraté de différentes façons, voir même généré par des logiciels spécialisés, soit exposé à ce que les commerçants continuent d'accepter les paiements non sécurisés. Enfin il existe la solution décrite dans le brevet US 005,883,810 consistant à fournir à l'acheteur à chaque transaction un nouveau code se substituant au code de sa carte de crédit, et de faire la correspondance à posteriori entre les deux codes. Cependant ce système reste une continuité de l'utilisation de la carte bancaire par correspondances, et par conséquent, comme dans le cas de l'utilisation d'un lecteur de carte, n'empêche pas l'utilisation frauduleuse d'un numéro de carte volé dans une base de donnée clients ou sur une facture de restaurant.

La présente invention propose un système de sécurisation des transmissions d'informations, et notamment lors de transactions lors d'achats par correspondance, qui permet de résoudre les problèmes précités.

Un autre but de l'invention est de proposer un système de transaction sécurisant aussi bien pour le client que pour le marchand.

L'invention a encore pour but un système évitant la transmission d'un code de carte bancaire via un réseau de communication.

On atteint les objectifs précités avec un système de transaction sécurisée via un réseau de communication, comprenant un terminal d'un client pour se connecter à ce réseau de communication et transmettre une requête d'achat, un serveur marchand pour recevoir la requête d'achat du client et une information de transaction fournie par le client, un serveur d'un tiers de confiance pour recevoir et valider l'information de transaction afin de procéder au paiement de l'achat. Selon l'invention, le

système comprend un module de traitement localisé chez le client et comprenant une table client qui renferme l'information de transaction, cette information de transaction étant unique pour chaque transaction. Par ailleurs, le serveur du tiers de confiance comprend un double de cette table client. La table client stockée dans le serveur du tiers de confiance est telle qu'elle est inaccessible par le réseau de communication. La requête d'achat peut comprendre un code d'identification du client tel que par exemple un numéro de série unique disposé sur le module de traitement.

Par module de traitement on entend un boîtier électronique ou tout autre module équipé de toute autre type de technologie telle que la technologie photonique, moléculaire ou mécanique.

De préférence, la table client comprend une série de numéros d'achat chacun associé à un numéro de certification unique. Avantageusement, chaque numéro de certification est un numéro aléatoire déterminé lors de la création de la table client. Suivant une variante de l'invention, la table comprend une série de numéros d'achat, et le boîtier électronique et le serveur du tiers de confiance comprennent un algorithme apte à déterminer pour chaque numéro d'achat un numéro de certification unique.

L'homme du métier pourra choisir entre telle ou telle version en fonction de la vitesse de calcul et de l'espace mémoire disponible dans le boîtier électronique. On peut choisir le type d'algorithme parmi les algorithmes de cryptographie existants dans la littérature tels que ceux décrits dans les documents US4405829 et FR2756122 par exemple, ou tout autre type d'algorithme. Il est cependant intéressant de choisir un algorithme de cryptage d'un degré suffisant pour que l'éventuel interception d'un

nombre important de codes ne permette pas à l'intercepteur de déterminer le code suivant. Si le concepteur du boîtier préfère utiliser un algorithme simple, il pourra alors limiter le nombre maximum de numéro d'achat sur un même boîtier, de façon à ce que la connaissance de la totalité de ces numéros d'achat ne permette pas de comprendre l'algorithme utilisé.

Avec un tel système, la transmission d'information, notamment pour une transaction par correspondance, est sécurisée. L'invention est particulièrement remarquable par le fait qu'on utilise un boîtier électronique contenant dans une mémoire une table client qui renferme une série de codes, ou information de transaction, correspondants à une série de requêtes de la part de l'utilisateur. Cette table client est connue et tenue secrète par un seul tiers de confiance qui peut avantageusement être la société émettrice du boîtier électronique. Idéalement, la mémoire est protégée de façon à ne pas être lisible par d'autre moyen que l'exécution du traitement prévu par la présente invention. Cette mémoire ne possède par exemple pas de connexions externes au boîtier, et/ou l'accès à ses connecteurs nécessite la destruction du boîtier. La table est donc isolée de tout système de communication externe.

Le tiers de confiance faisant office d'établissement de crédit ou de banque ou étant associée à un établissement de crédit ou bancaire, est garante de la validité de la transaction.

Le boîtier électronique possède un ou plusieurs circuits logiques, typiquement un microprocesseur, ayant en charge d'une part la gestion interne des informations et d'autre part les calculs nécessaires aux différents traitements. Selon une caractéristique de l'invention, le boîtier comprend en outre des moyens de traitement pour

fournir à chaque sollicitation un nouveau numéro d'achat ainsi qu'un nouveau numéro de certification associé. En particulier, ces moyens de traitement peuvent comprendre un compteur incrémental s'incrémentant d'une unité à chaque fourniture d'un numéro de certification, et le numéro d'achat peut avantageusement être la valeur de ce compteur incrémental. Le serveur du tiers de confiance possède également un tel compteur.

Le boîtier électronique peut comprendre en outre une interface homme/machine. Cette interface homme machine peut être composée d'une part d'un élément d'acquisition, par exemple un clavier de dix touches allant de 0 à 9 plus éventuellement deux touches programmables, par exemple "Validation" et "Annulation", ou bien par exemple un micro associé à un circuit de reconnaissance et d'analyse vocale, ou d'une façon générale tout type d'acquisition de données pour la machine. Le boîtier électronique peut aussi comprendre un écran de visualisation, ou tout type de composant permettant de transmettre des informations à l'utilisateur, voire un écran tactile faisant en même temps office de clavier d'acquisition. On peut également prévoir des moyens de verrouillage et de déverrouillage de l'accès à la table client, le déverrouillage étant obtenu au moyen d'un code secret ou code "PIN" (PERSONAL IDENTIFICATION NUMBER, en langue anglaise).

Le format de la carte de crédit est si répandu et si adapté à la vie quotidienne, qu'il est préférable que le boîtier électronique présente un tel format. Cependant, comme une interface homme/machine est nécessaire, on préconisera l'utilisation d'une carte ayant un clavier sensitif, ou de toute technologie de faible épaisseur, de 12 touches (0 à 9, "valider", "annuler"), et un écran digital, une telle carte ayant par ailleurs déjà été décrite dans la littérature (FR 2 768 532).

Le boîtier électronique ne nécessitant en premier lieu pas de communication électronique extérieure, l'interface de communication par contact affleurant habituel sur les cartes à puces bancaires n'est pas nécessaire. Cette interface pourra cependant apparaître dans le cas d'une carte hybride supportant d'autres fonctions que celles exposées précédemment. Il faudra alors prendre soin de conserver l'inviolabilité de la mémoire contenant la table client soit par une séparation physique des circuits à l'intérieur du boîtier, soit par une séparation électronique de ces circuits. Il pourra toutefois exister une zone de contacts affleurants, géographiquement bien définie sur le boîtier électronique, comprenant deux pôles afin, soit d'alimenter le boîtier en électricité pour son fonctionnement, soit de recharger une batterie d'alimentation interne au boîtier. L'alimentation électrique par cellule photoélectrique, ou par champ induit, est également possible.

Suivant un autre aspect de l'invention, il est proposé un procédé de transaction sécurisée via un réseau de communication, dans lequel un client se connecte, via un terminal, à un serveur marchand en vue de réaliser un achat. Selon l'invention, le procédé comprend les étapes de :

- génération d'une information de transaction à partir d'une table client stockée dans un boîtier électronique en possession du client, cette table étant isolée du réseau de communication,
- transmission, par exemple via le terminal, de l'information de transaction vers un serveur d'un tiers de confiance, ce serveur du tiers de confiance renfermant un double de la table client,
- réception de l'information de transaction par le serveur du tiers de confiance et comparaison de cette

information avec la table client stockée dans ce serveur du tiers de confiance,

- validation de l'achat lorsque la comparaison est positive.

La comparaison est positive lorsque l'information de transaction est contenue dans la table client stockée dans le serveur du tiers de confiance et le serveur du tiers de confiance reçoit cette information de confiance pour la première fois. En d'autres termes, la comparaison est positive lorsque le serveur du tiers de confiance reçoit un numéro d'achat et un numéro de certification non encore utilisés. Plus précisément, cette comparaison consiste à vérifier si pour un numéro d'achat contenu dans l'information de transaction reçue, le numéro de certification associé est identique à celui contenu dans la table client stockée dans ce serveur du tiers de confiance.

Selon l'invention, le serveur du tiers de confiance notifie au client le résultat de la comparaison.

D'autres avantages et caractéristiques de l'invention apparaîtront à l'examen de la description détaillée d'un mode de mise en œuvre nullement limitatif, et des dessins annexés sur lesquels :

- la figure 1 est un schéma simplifié illustrant les principaux éléments du système ainsi que le parcours des informations échangées;

- la figure 2 est un schéma-bloc illustrant quelques éléments constitutifs d'un boîtier électronique selon l'invention;

- la figure 3 est un organigramme des étapes d'obtention d'un numéro d'achat et d'un numéro de certification selon l'invention; et

- la figure 4 est un schéma-bloc illustrant l'intégration du boîtier électronique dans un téléphone portable.

Sur la figure 1 on distingue trois principales entités, le client 10, le marchand 30 et la banque 20 qui fait office de tiers de confiance. Ces trois entités sont connectées au réseau de communication Internet au moyen, respectivement, d'un micro-ordinateur 40, d'un serveur-marchand 60 et d'un serveur-banque 50. Le client 10 possède avantageusement un boîtier électronique 70 délivré par la banque 20. Quelques éléments de ce boîtier sont représentés sur la figure 2.

On distingue, sur cette figure 2, dans le boîtier électronique 70 une table client 80 formée de deux colonnes, une colonne "N° d'achat" composée d'une série de numéros allant de 1 à 999 et une colonne "N° de certification" composé d'une série de codes prédéterminés de façon aléatoire et unique. Le boîtier comprend également un circuit logique 110 comportant au moins un microcontrôleur ou un microprocesseur, et une interface homme/machine 120 incluant notamment un écran 130 et un clavier 140. Un numéro de série 100 est disposé sur un côté de ce boîtier de façon à rester constamment visible. Avantageusement, comme on peut le voir sur la figure 1, le boîtier électronique et le serveur-banque possèdent tous deux une même table client 80. Cette table client est stockée dans le serveur 50 de façon à être inaccessible à travers Internet. Le boîtier électronique présente un format proche d'une carte de crédit conventionnelle et possède un clavier sensitif et un écran digital, une telle carte ayant par ailleurs déjà été décrite dans la littérature (FR 2 768 532).

On va maintenant décrire une procédure de transaction selon l'invention en se référant en particulier à la figure 1.

Le client 10, se met en contact au moyen du micro-ordinateur 40 avec le serveur 60 du marchand 30. La notion de client et de marchand peut être élargie à toute relation de transmission mettant en relation un parti émettant une information signée et un parti désireux de recevoir cette information avec l'assurance que la signature désigne effectivement le parti émetteur. Le client a accès au serveur du marchand via le réseau Internet. On suppose qu'il a déjà choisi une marchandise qu'il désire acquérir. Pour le règlement de son achat, le marchand 30 demande alors au client 10 de transmettre un identifiant, lequel peut être par exemple son nom si celui-ci est suffisamment unique, ou un identifiant défini à l'avance avec le tiers de confiance 20 qui est une banque. A titre d'exemple, cet identifiant est le numéro de série 100 du boîtier électronique 70, lequel est unique et noté sur le dit boîtier. Le marchand demande également un numéro d'achat et un numéro de certification, lequel peut être un code numérique ou alphanumérique ou alphabétique.

A l'étape 1 sur la figure 1, le client se fait reconnaître auprès de son boîtier électronique par l'introduction d'un code de signature individuel, par exemple sous la forme d'un code à 4 chiffres, communément nommé code PIN (Personal Identification Number). Le boîtier électronique possède un composant de surveillance vérifiant la validité de ce code, et gérant par un blocage momentané ou définitif son utilisation après un nombre définit d'erreurs d'introduction, par exemple après trois essais infructueux successifs.

Après validation du code PIN, le système électronique délivre au client un numéro d'achat issu d'un compteur interne. Ce numéro s'incrémente d'une unité chaque fois que le client accède à un numéro de certification. Il correspond donc au nombre d'achats, ou de demandes de numéros de certification, effectué par le client.

La table client enregistrée dans la mémoire du boîtier électronique fait correspondre à chacun des numéros d'achat un numéro de certification défini aléatoirement lors de l'initialisation du boîtier par la banque.

Le client introduit à l'étape 2 son identifiant, le numéro d'achat ainsi que le numéro de certification délivrés par le boîtier électronique 70 dans son micro-ordinateur 40 de façon à les transmettre à l'étape 3 vers le serveur 60 du marchand 30. Ce triplet peut par exemple être constitué respectivement des données : "1234" pour l'identifiant; "004" pour le numéro d'achat; et "43B1" pour le numéro de certification. Cette transmission est de préférence sécurisée au moyen de techniques conventionnelles. Le marchand établit alors une facture 90 comprenant le triplet transmis par le client ainsi que des informations concernant la marchandise désirée par le client, par exemple le prix de cette marchandise. A l'étape 4, le marchand prend contact avec la société émettrice du système en lui fournissant la facture 90 à travers Internet de façon sécurisée à l'aide de techniques connues. La banque vérifie la validité de ces informations à l'aide du double de la table client qu'elle possède et enregistre l'utilisation de ce numéro d'achat. Elle fournit au marchand, à l'étape 5, un accord de transaction lorsque, pour le client identifié au moyen de l'identifiant "1234" et pour le numéro d'achat "004", le numéro de certification "43B1" correspond bien au numéro

de certification présent dans la table client stockée dans le serveur 50. Au préalable, la banque a bien pris soin de vérifier que pour ce client, le numéro d'achat est utilisé pour la première fois. La banque peut également effectuer directement le paiement de la commande depuis le compte du client, et éventuellement envoyer à l'étape 6, par exemple par messagerie électronique, un reçu au client. Si ultérieurement la banque reçoit une facture d'achat comprenant un numéro d'achat ou un numéro de certification déjà utilisé, elle refusera cette facture, et éventuellement en avertira, par exemple par messagerie électronique, ou tout autre moyen, le client identifié.

Lorsque le marchand reçoit l'accord de la banque à l'étape 5, il peut alors transmettre la marchandise commandée par le client à l'étape 7.

La durée entre l'instant où le client transmet l'information (numéro de série, numéro d'achat, numéro de certification), et celui où la banque enregistre cette utilisation devra être la plus courte possible. Ainsi si cette durée reste inférieure au temps nécessaire à son utilisation frauduleuse, on pourra parler de sécurité absolue du système. On peut intégrer dans la transaction une estampille temporelle de type "TSA" ("Time Stamping Authority" en langue anglaise, une technologie en étude à l'ETSI, European Telecommunications Standards Institute, ETSI TS 101 861, http://www.etsi.org). Cette estampille est introduite de façon cryptée, au moyen du micro-ordinateur du client, dans l'information de transaction à destination du serveur de la banque. A la réception, le serveur de la banque décrypte l'estampille, la compare aux données temporelles réactualisées d'un serveur "TSA" par exemple, et peut ainsi produire une erreur sur la transaction pour délai écoulé si la durée écoulée entre

transmission et réception semble dépasser une durée de transmission normale prédéfinie.

La figure 3 est un organigramme débutant à l'étape 150 et illustrant différentes étapes nécessaires pour accéder au numéro d'achat et au numéro de certification, ces étapes étant réalisées par le circuit logique 110 du boîtier électronique. A l'étape 170, la variable "x", par exemple égale à 3 à l'étape 150, représente le nombre maximum d'essais d'introduction d'un code PIN erronés. Si "x" est égale à zéro, le circuit logique affiche à l'étape 160 "erreur code PIN" et se bloque. Un éventuel déblocage nécessite l'intervention de la société émettrice, à savoir la banque 20.

Lorsque "x" est différent de zéro, le client peut introduire son code PIN et appuyer sur la touche "Validation" à l'étape 180. Le circuit logique compare alors ce code PIN avec un code pré-chargé à l'étape 190. Si le code PIN n'est pas le bon, on passe à l'étape 200 en décrémentant la variable "x" d'une unité, puis on retourne à l'étape 170.

Lorsque le code PIN est exact, on affiche à l'étape 210 le numéro d'achat et le numéro de certification. Puis, le circuit logique respecte un délai de cinq minutes qui peut être interrompu par un appui sur la touche "Annulation". Après ce délai, le circuit logique incrémente le numéro d'achat d'une unité à l'étape 230, puis vérifie à l'étape 240 si ce numéro est égal à 999 qui représente la dernière valeur possible du numéro d'achat dans la table client. Lorsque le numéro d'achat a atteint la valeur 999, on affiche à l'étape 250 "carte expirée" et le circuit logique se bloque, dans le cas contraire on se place au début de la procédure en 150.

Le boîtier électronique peut être un téléphone portable ou un agenda électronique personnel, au sein

duquel a été placé l'ensemble circuit logique\table client. Cependant, de préférence, dés lors qu'on utilise comme interface un appareil ayant la possibilité d'être connecté à un réseau de communication, on prendra particulièrement soin de conserver la stricte impossibilité de lecture des données de la table par un quelconque accès externe au support en dehors de l'interface homme-machine prévu précédemment. Comme on le voit sur la figure 4, on utilise un téléphone portable 260 comme un simple lecteur dans lequel on a placé un module de transaction 290 contenant la table client 80, un identifiant 300 ainsi que le circuit logique 110 capable de piloter les étapes illustrées sur la figure 3. L'interface homme-machine 270 est, soit en communication avec le module de transaction 290, soit en communication avec un module téléphonique 280 nécessaire pour réaliser au moins la fonction de téléphonie mobile. Le téléphone n'apporte qu'une interface homme-machine. Lorsque le client exécute le processus d'obtention du numéro d'achat et du numéro de certification, ces deux numéros peuvent être mémorisés par le client ou de préférence stockés dans une mémoire tampon. Ensuite, une fois le téléphone connecté au réseau sans fil, on peut transmettre les numéros d'achat et de certification à partir de cette mémoire tampon.

La transmission de données (numéro de série / numéro d'achat / numéro de certification) peut donc se faire en utilisant un réseau téléphonique filaire ou non sous forme d'un signal numérique.

Bien sûr, l'invention n'est pas limitée aux exemples qui viennent d'être décrits et de nombreux aménagements peuvent être apportés à ces exemples sans sortir du cadre de l'invention, notamment on peut utiliser le système selon l'invention pour des traitements autres que l'achat

de marchandise, par exemple des traitements pour la transmission d'information, pour un échange de contrat nécessitant une authentification... On peut aussi envisager un mode automatique entre par exemple un serveur marchand et un serveur client, le serveur client ayant accès à un programme de délivrance des numéros d'achat et de certification indépendamment de la connexion avec le réseau de communication.

REVENDICATIONS

1. Système de transaction sécurisée via un réseau de communication, comprenant un terminal (40) d'un client (10) pour se connecter audit réseau de communication et transmettre une requête d'achat, un serveur marchand (60) pour recevoir la requête d'achat du client et une information de transaction fournie par le client (10, 40), un serveur (50) d'un tiers de confiance (20) pour recevoir et valider l'information de transaction afin de procéder au paiement de l'achat, caractérisé en ce qu'il comprend un module de traitement (70) localisé chez le client et comprenant une table client (80) qui renferme l'information de transaction, cette information de transaction étant unique pour chaque transaction, et en ce que le serveur du tiers de confiance comprend un double de cette table client (80).

2. Système selon la revendication 1, caractérisé en ce que la table client (80) comprend une série de numéros d'achat chacun associé à un numéro de certification unique.

3. Système selon l'une des revendications 1 et 2, caractérisé en ce que le module de traitement (70) comprend en outre des moyens de traitement (110) pour fournir à chaque sollicitation un nouveau numéro d'achat ainsi qu'un nouveau numéro de certification associé.

4. Système selon l'une des revendications 2 et 3, caractérisé en ce que chaque numéro de certification est un numéro aléatoire déterminé lors de la création de la table client.

5. Système selon la revendication 1, caractérisé en ce que la table client (80) comprend une série de numéros d'achat et en ce que le module de traitement (70) et le serveur (50) du tiers de confiance (20) comprennent en outre un algorithme apte à déterminer pour chaque numéro d'achat un numéro de certification unique.

6. Système selon l'une quelconque des revendications 2 à 5, caractérisé en ce que le module de traitement (70) et le serveur (50) du tiers de confiance comprennent un compteur incrémental s'incrémentant d'une unité à chaque fourniture d'un numéro de certification, et en ce que le numéro d'achat est la valeur de ce compteur incrémental.

7. Système selon l'une quelconque des revendications précédentes, caractérisé en ce que la table client (80) est isolée de tout système de communication externe.

8. Système selon l'une quelconque des revendications précédentes, caractérisé en ce que le module de traitement (70) comprend des moyens de verrouillage et de déverrouillage de l'accès à la table client, le déverrouillage étant obtenu au moyen d'un code secret.

9. Système selon l'une quelconque des revendications précédentes, caractérisé en ce que la requête d'achat comprend un code d'identification du client.

10. Système selon la revendication 9, caractérisé en ce que le module de traitement comprend un numéro de série (100) unique servant de code d'identification du client.

11. Système selon l'une quelconque des revendications précédentes, caractérisé en ce que le module de traitement

comprend au moins un clavier (140) de dix touches numérotées de 0 à 9, et deux touches permettant des fonctions de validation et annulation.

12. Système selon l'une quelconque des revendications précédentes, caractérisé en ce que le module de traitement comprend un écran de visualisation (130).

13. Système selon l'une quelconque des revendications précédentes, caractérisé en ce que le module de traitement comprend un écran tactile.

14. Système selon l'une quelconque des revendications précédentes, caractérisé en ce que le module de traitement se présente sous le format d'une carte de crédit conventionnelle.

15. Système selon l'une quelconque des revendications 1 à 13, caractérisé en ce que le module de traitement est un téléphone portable (260).

16. Système selon l'une quelconque des revendications 1 à 13, caractérisé en ce que le module de traitement est un agenda électronique.

17. Système selon l'une quelconque des revendications précédentes, caractérisé en ce que le tiers de confiance est une banque.

18. Procédé de transaction sécurisée via un réseau de communication, dans lequel un client (10) se connecte, via un terminal (40), à un serveur marchand (60) en vue de réaliser un achat, caractérisé en ce qu'il comprend les étapes de :

- génération d'une information de transaction à partir d'une table client (80) stockée dans un module de traitement (70) en possession du client, cette table étant isolée du réseau de communication,
- transmission de l'information de transaction vers un serveur (50) d'un tiers de confiance (20), ce serveur du tiers de confiance renfermant un double de la table client (80),
- réception de l'information de transaction par le serveur du tiers de confiance et comparaison de cette information avec la table client stockée dans ce serveur du tiers de confiance,
- validation de l'achat lorsque la comparaison est positive.

19. Procédé selon la revendication 18, caractérisé en ce que la comparaison est positive lorsque l'information de transaction est contenue dans la table client stockée dans le serveur du tiers de confiance et le serveur du tiers de confiance reçoit cette information de confiance pour la première fois.

20. Procédé selon l'une des revendications 18 et 19, caractérisé en ce qu'on génère l'information de transaction en prélevant dans la table client stockée dans le module de traitement un numéro d'achat associé à un numéro de certification.

21. Procédé selon la revendication 20, caractérisé en ce que la comparaison est positive lorsque le serveur du tiers de confiance reçoit un numéro d'achat et un numéro de certification non encore utilisés.

22. Procédé selon l'une des revendications 20 et 21, caractérisé en ce que la comparaison consiste à vérifier si pour un numéro d'achat contenu dans l'information de transaction reçue, le numéro de certification associé est identique à celui contenu dans la table client stockée dans ce serveur du tiers de confiance.

23. Procédé selon l'une quelconque des revendications 20 à 22, caractérisé en ce qu'on incrémente le numéro d'achat de telle sorte que pour chaque sollicitation du module de traitement on génère un nouveau numéro d'achat.

24. Procédé selon l'une quelconque des revendications 18 à 23, caractérisé en ce qu'on transmet l'information de transaction accompagnée d'un code d'identification permettant d'identifier le client.

25. Procédé selon la revendication 24, caractérisé en ce qu'on détermine le code d'identification du client à partir d'un numéro de série (100) du module de traitement.

26. Procédé selon l'une quelconques des revendications 18 à 25, caractérisé en ce que l'information de transaction transite (3, 4) par le serveur marchand qui le transmet au serveur du tiers de confiance.

27. Procédé selon l'une quelconque des revendications 18 à 26, caractérisé en ce que la table client comprend une série de numéros d'achat de telle sorte qu'on détermine à partir de chaque numéro d'achat un numéro de certification unique au moyen d'un algorithme

28. Procédé selon l'une quelconque des revendications 18 à 27, caractérisé en ce que le serveur du tiers de confiance notifie (6) au client le résultat de la comparaison.

29. Procédé selon l'une quelconque des revendications 18 à 28, caractérisé en ce que l'information de transaction comprend en outre une estampille permettant au serveur du tiers de confiance de déterminer la durée entre la transmission et la réception de cette information de transaction.

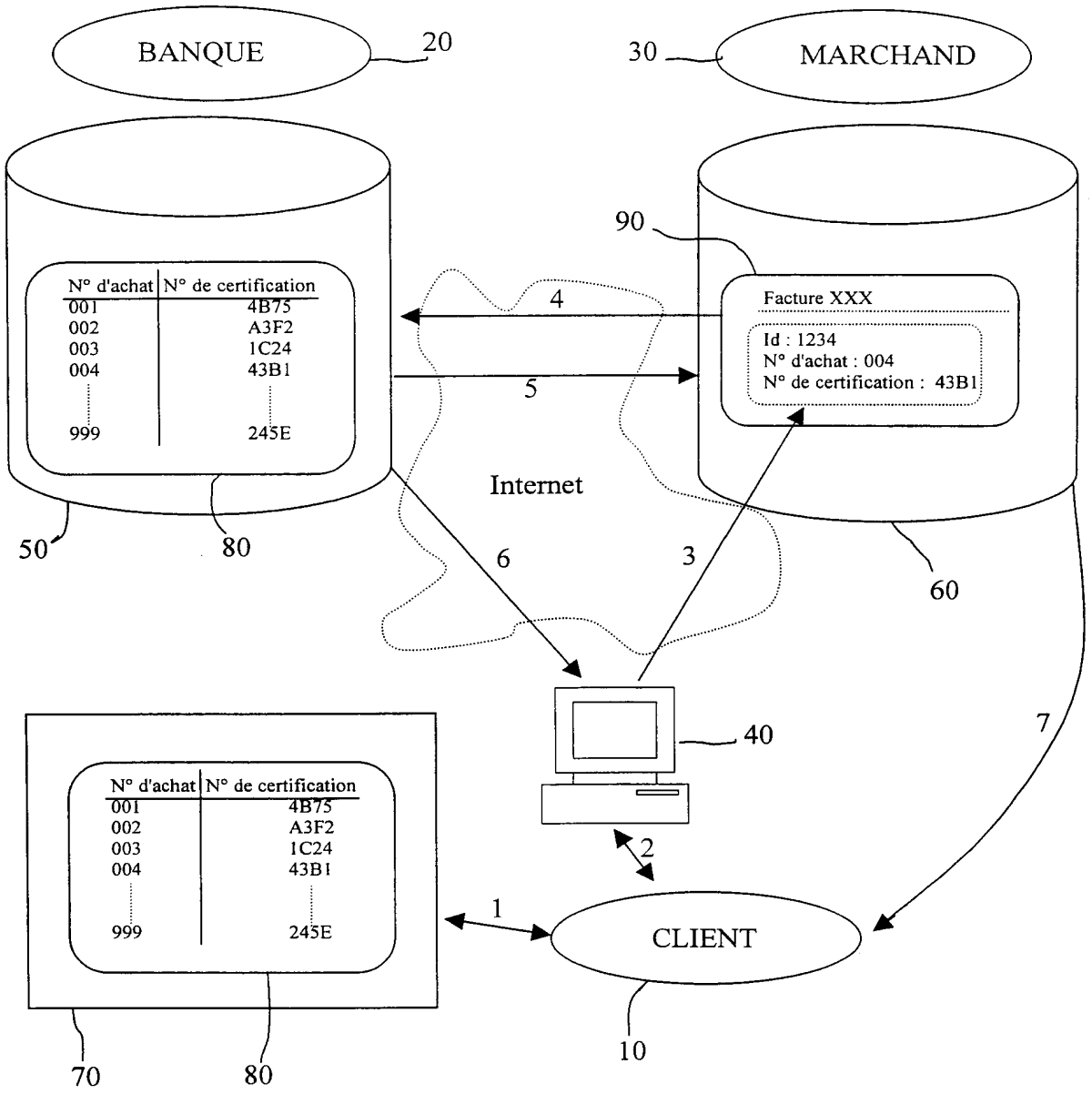

BANQUE
20
30
MARCHAND
90
N° d'achat
N° de certification
001
4B75
002
A3F2
003
1C24
004
43B1
999
245E
4
5
Facture XXX
Id : 1234
N° d'achat : 004
N° de certification : 43B1
Internet
50
80
6
3
60
40
7
2
1
CLIENT
10
70
80

FIGURE 1

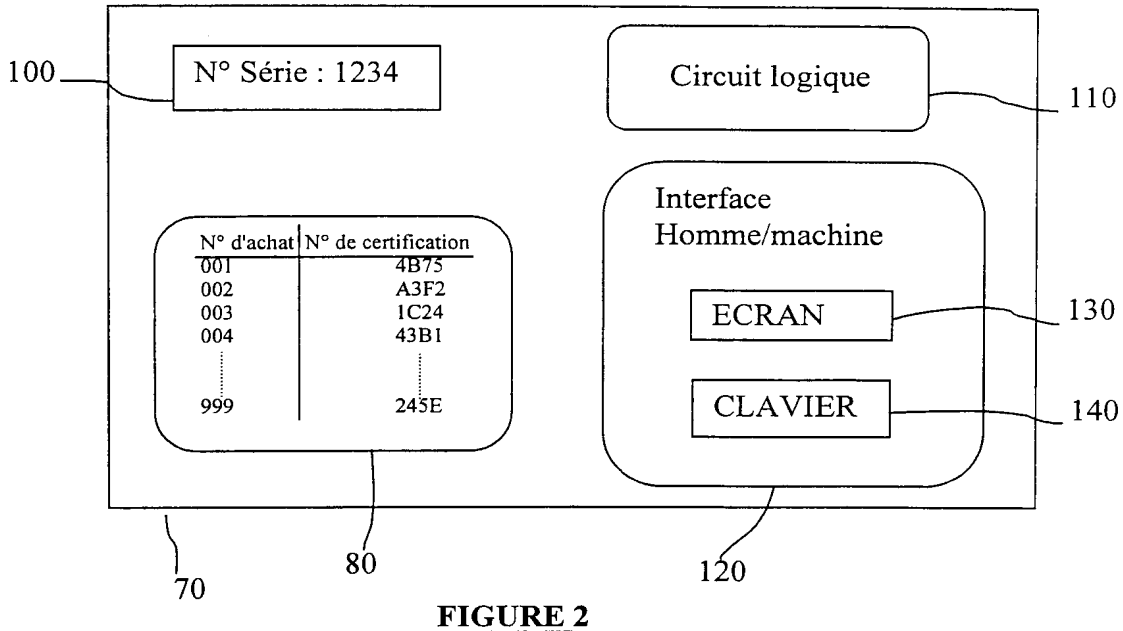


FIGURE 2

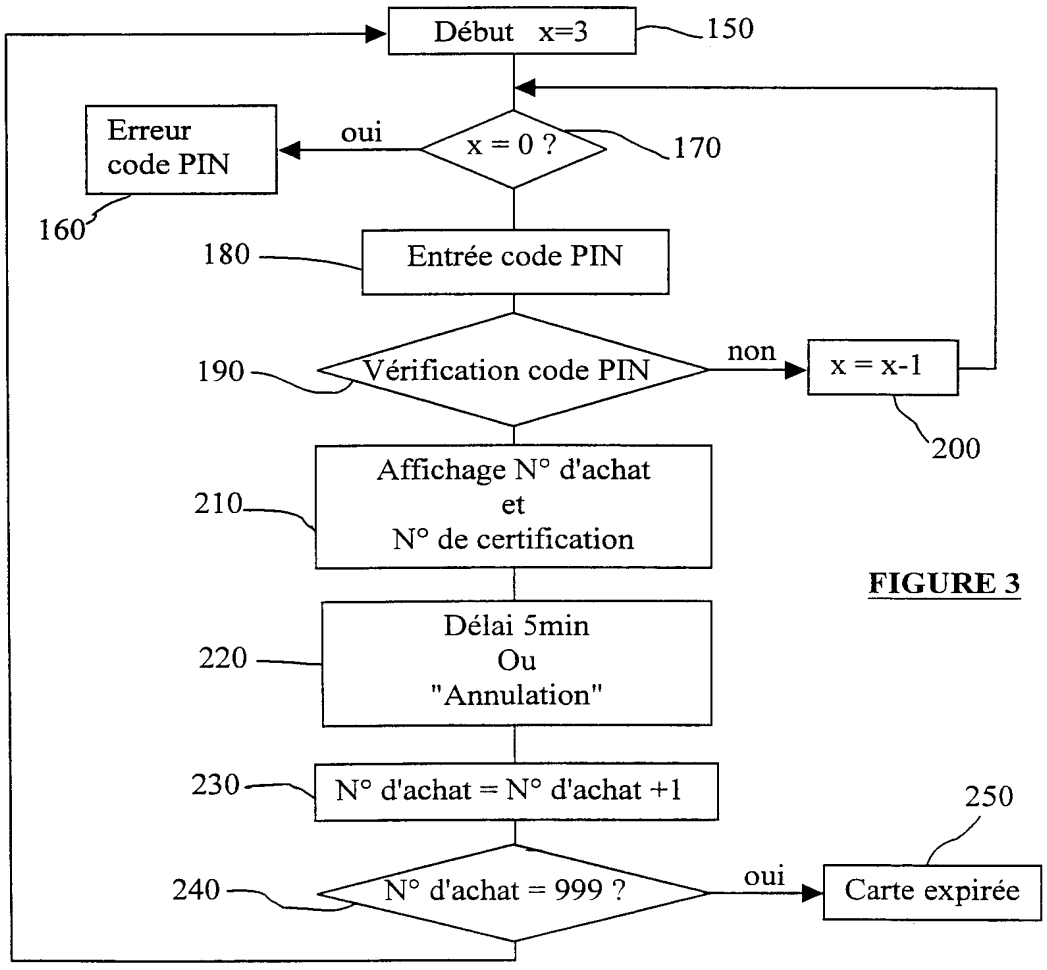


FIGURE 3

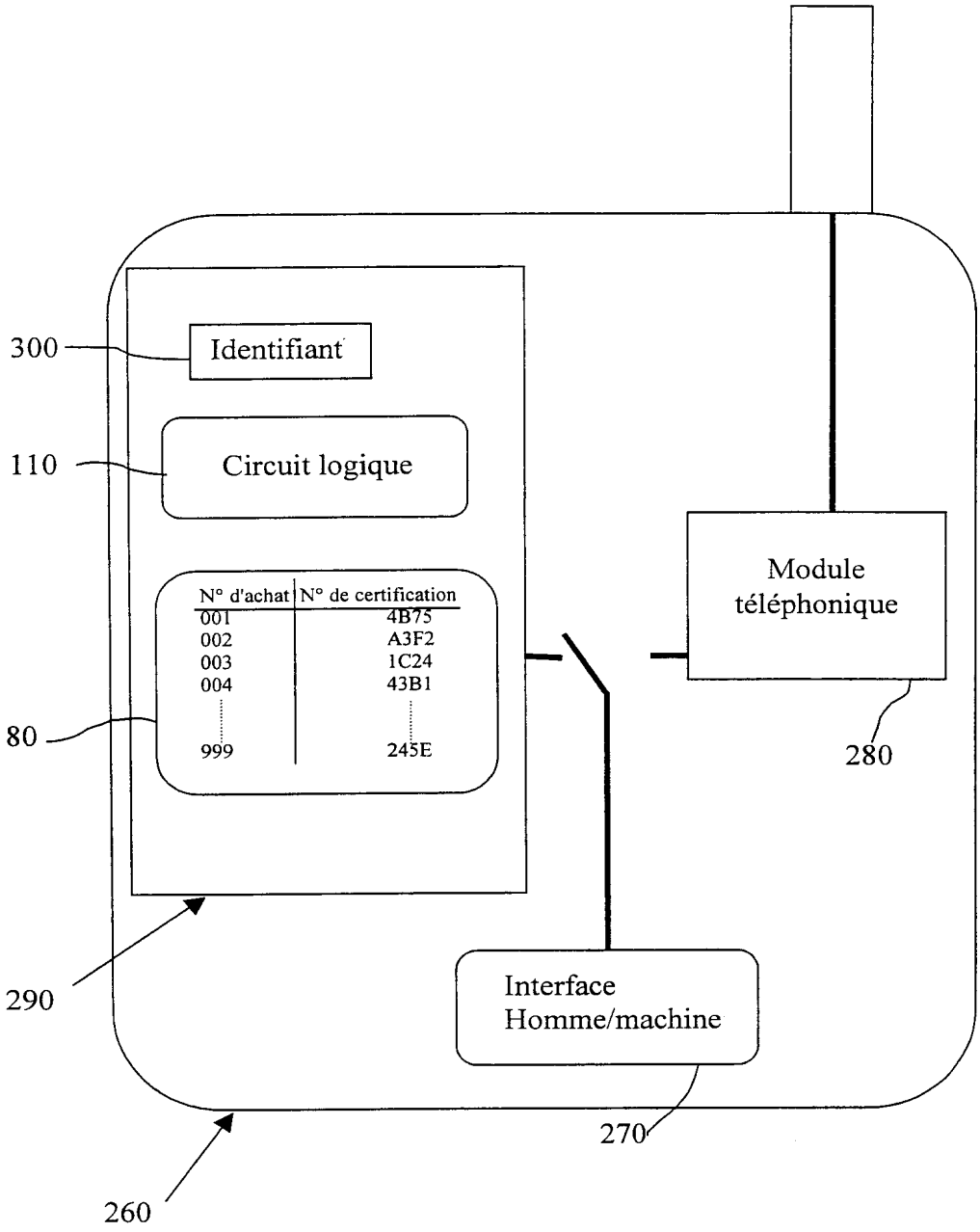

300
Identifiant
110
Circuit logique
N° d'achat
N° de certification
001
4B75
002
A3F2
003
1C24
004
43B1
999
245E
80
Module téléphonique
280
290
Interface Homme/machine
270
260

FIGURE 4